APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/598,719	09/08/2006	Agostinho De Arruda Villela	2171323-000002	9289

44777   7590   09/09/2010
W. EDWARD RAMAGE
COMMERCE CENTER SUITE 1000
211 COMMERCE ST
NASHVILLE, TN 37201

EXAMINER
WRIGHT, BRYAN F

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
09/09/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eramage@bakerdonelson.com

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/598,719	DE ARRUDA VILLELA, AGOSTINHO
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>6/14/2010</u>.

2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>17-35</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>17-35</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

``DETAILED ACTION

In view Appellant's Appeal Arguments filed 6/14/2010, PROSECUTION IS
HEREBY REOPENED. A new ground(s) of rejection cited under prior art references
Moshir, Bajika, Nishibi, Hyman, Cui and Abburi are set forth below. To avoid
abandonment of the application, appellant must exercise one of the following two
options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply
under 37 CFR 1.113 (if this Office action is final); or,(2) initiate a new appeal by filing a
notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37.
The previously paid notice of appeal fee and appeal brief fee can be applied to the new
appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased
since they were previously paid, then appellant must pay the difference between the
increased fees and the amount previously paid. A Supervisory Patent Examiner (SPE)
has approved of reopening prosecution by signing below. Claims 17-35 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all
obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set
forth in section 102 of this title, if the differences between the subject matter sought to be patented and
the prior art are such that the subject matter as a whole would have been obvious at the time the
invention was made to a person having ordinary skill in the art to which said subject matter pertains.
Patentability shall not be negatived by the manner in which the invention was made.

1.   Claims 17, 18, 19, 22, 23, 26-28, 31 and 33-35 are rejected under 35 U.S.C.

103(a) as being unpatentable over Moshir (US Patent Publication 2004/0003266) in

view of Bajikar (US Patent Publication 2005/0133582) and further in view of Nishibi (US

Patent Publication 2005/0076096).

2.   As for claims 17, 31 and 34, Moshir teaches a method for identifying devices and

controlling access to a service comprises: collecting (e.g., gathers) data related to

software and hardware configurations from a device through a software agent (i.e.,

…teaches a discover agent gathers information about the target computer such as

hardware and software configurations [par. 92]);

        determining whether the device has been excluded from accessing or enrolling in

the service (i.e., ... the Examiner notes that applicant states in paragraph 9 of

applicant's original disclosure that the term "service" relates to access to an Internet

page, an Intranet page, or any other type of computer server or computer-based

service. The Examiner contends that Moshir discloses in paragraph 81 an enrollment

process for indicating a desired level of participation. A preferred embodiment of the

invention has three different user levels: guest, regular, and executive. A guest is

allowed to view a web site. The Examiner adds that all participation is through a user's

target computer (e.g., device) and that it is understood that the depending on how the

user and target computer was enrolled, that access permission to web sites (e.g.,

computer based services) would be control accordingly.)

Moshir doesn't specifically disclose generating a digital signature for the device

by hashing the software and hardware configuration data. However at the time of

applicant's original filings prior art reference Bajikar discloses attestation may be

accomplished by digitally signing a digest value of the piece of data that is to be

attested. For a more complex implementation, the digest value may be synthesized by

combining together various other elements in addition to the original data to be attested.

Examples of such elements may include, but not be limited to, hash values of platform

hardware/software configuration, other credentials, one-time nonce values, etc

(Paragraph 55). Therefore, to enhance the device authentication and access control

capabilities of Moshir, a person of ordinary skill in the art at the time the invention would

have modify Moshir with Bajikar's capability to generate a device digital signature

thereby affording Moshir a means to more comprehensively authenticate a device

within the device registration/management process.

Both Moshir and Bajikar do not expressing disclose sending the digital signature of the

device to an authentication server. However at the time of applicant's original filing,

prior reference Nishibi disclosed a signature is transmitted to the EMD server

(authentication server). See Nishibi paragraph. 227. Therefore, to enhance the device

authentication process of both Moshir and Bajikar, a person of ordinary skill in the art at

the time of the invention would have modified the combined teachings of Moshir and

Bajikar with Nishibi's capability to transmit a digital signature to an authentication server

(e.g., EMD sever) for authentication.

3.   As for claim 18, Moshir teaches a method where the digital signature sent to the
authentication server is encrypted (i.e., ... teaches that a signature may also be
encrypted [par. 109]).

4.   As for claim 19, Moshir teaches a method where the software agent is installed
on the device as part of the process of using the device to access a service (i.e.
...teaches discover agent is installed on the hardware and software of the target
computer [par. 23]).

5.   As for claim 22, Moshir teaches a method where the authentication server
compares the digital signature sent with one or more previously- stored digital
signatures (i.e., ...teaches comparing previous information (i.e. signature) stored in
library [par. 91]).

6.   As for claim 23, Moshir teaches a method where the authentication server
determines whether the device has been excluded from accessing or enrolling in the
service by determining whether the device is on a list or in a group of devices not
allowed to access the service, or is included within a group of devices allowed to access
the service (i.e., ...teaches update server 528 can present the user with detailed reports
of the current patch status for all computers within the network [par. 24]).

7.   As for claim 26, Moshir teaches a method where the authentication server allows

minor modifications to the software or hardware configurations of a previously-enrolled

device so as to preserve access or denial of access for the device (i.e., …teaches

discloses hardware information including specific software updates with configurations

[par. 99]).

8.   As for claim 27, Moshir teaches a method where the previously-stored digital

signature of the device is updated to reflect the modifications (i.e., …teaches signature

updates [par. 109 & 185]).

9.   As for claim 28, Moshir teaches a method where the authentication server logs

all accesses or attempted accesses by a device to the service (i.e., …teaches the

update server can drill through the firewall to access the target computer [par. 61]).

10.   As for claim 33, Moshir teaches a where the step of registering a device

comprises the steps of (see abstract): collecting (e.g., gathers) data related to software

and hardware configurations from a device through a software agent (i.e., …teaches a

discover agent gathers information about the target computer such as hardware and

software configurations [par. 92]);

        comparing the digital signature sent with one or more previously-stored digital

signatures for the device (i.e., …teaches a comparing previous information (i.e.

signature) stored in library) [par. 91]).

Moshir doesn't specifically disclose generating a digital signature for the device by hashing the software and hardware configuration data. However at the time of applicant's original filing, prior art reference Bajikar discloses attestation may be accomplished by digitally signing a digest value of the piece of data that is to be attested. For a more complex implementation, the digest value may be synthesized by combining together various other elements in addition to the original data to be attested. Examples of such elements may include, but not be limited to, hash values of platform hardware/software configuration, other credentials, one-time nonce values, etc. See Bajikar paragraph 55. Therefore, to enhance the device authentication capabilities of Moshir, a person of ordinary skill in the art at the time of the invention would have modified Moshir with Bajikar's capability to generate a device digital signature thereby affording Moshir a means to more comprehensively authenticate a device within the device registration/management process.

Both Moshir and Bajikar do not expressing disclose sending the digital signature of the device to an authentication server. However at the time of applicant's original filing, prior reference Nishibi disclosed a signature is transmitted to the EMD server (authentication server). See Nishibi paragraph. 227. Therefore, to enhance the device authentication process of both Moshir and Bajikar, a person of ordinary skill in the art at the time of the invention would have modified the combined teachings of Moshir and

Bajikar with Nishibi's capability to transmit a digital signature to an authentication server

(e.g., EMD sever) for authentication.

11.   As for claims and 35, Moshir discloses a method for identifying devices and

controlling access to a service, comprising the steps of (see abstract): collecting data

related to software and hardware configurations from a device through a software agent

(i.e., ..teaches a discover agent gathers information about the target computer such as

hardware and software configurations [par. 92]);

Moshir doesn't specifically disclose generating a digital signature for the device by

hashing the software and hardware configuration data. Bajikar discloses attestation may

be accomplished by digitally signing a digest value of the piece of data that is to be

attested. For a more complex implementation, the digest value may be synthesized by

combining together various other elements in addition to the original data to be attested.

Examples of such elements may include, but not be limited to, hash values of platform

hardware/software configuration, other credentials, one-time nonce values, etc. See

Bajikar paragraph 55. Therefore, it would have been obvious to one of ordinary skill in

the art at the time the invention was made to modify Moshir by generating a digital

signature for the device by hashing the software and hardware configuration data, as

taught by Bajikar. The motivation would have been to provide an improved digital

signature generation process.

Both Moshir and Bajikar do not expressing disclose sending the digital signature of the device to an authentication server. However at the time of applicant's original filing, prior reference Nishibi disclosed a signature is transmitted to the EMD server (authentication server). See Nishibi paragraph. 227. Therefore, to enhance the device authentication process of both Moshir and Bajikar, a person of ordinary skill in the art at the time of the invention would have modified the combined teachings of Moshir and Bajikar with Nishibi's capability to transmit a digital signature to an authentication server (e.g., EMD sever) for authentication.

12.   Claims 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moshir and Bajika in view of Nishibi, as applied to claim 17 above, and further in view of Cui (US Patent Publication 2005/0166053).

13.   As for claim 20, the system of Moshir and Bajikar in view of Nishibi discloses a method for generating a signature device, however their system does not specifically disclose wherein the hashes used to generate the digital signature are changed with every attempt to access a service, and the hashes cannot be reversed. However at the time of applicant original filing, prior art reference Cui discloses making a determination on whether the device signature(s) are to be rolled over; updating (rolling) the device signature(s) based, in part, on a pre-determined period of time. See Cui paragraph 63 and 70. Therefore, to enhance signature data security/integrity, a person of ordinary skill in the art at the time of the invention would have modified the system of Moshir and

Bajikar in view of Nishibi with Cui's disclosed method of hashes used to generate the

digital signature which are changed with every attempt to access a service, and the

hashes cannot be reversed.

14.   As for claim 21, Moshir in view of Bajikar discloses the method where the digital

signature sent to the authentication server is encrypted (i.e., …teaches signature

information sent to the updated server). See Moshir paragraph 109. Moshir in view of

Bajikar doesn't specifically disclose wherein the digital signature is one of several

stages of a framework of authorization and authentication processes governing access

to the service by the device. However prior art reference Cui discloses determining at

least one device signature for a mobile device (See fig. 3; Paragraph 51, 52).

Therefore, to enhance the authorization process of Moshir and Bajikar in view of Nishibi,

a person of ordinary skill in the art at the time of the invention would have modified the

system of Moshir and Bajikar in view of Nishibi with Cui's disclosed method wherein the

digital signature is one of several stages of a framework of authorization and

authentication processes governing access to the service by the device, and the hashes

cannot be reversed.

15.   Claims 24 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Moshir and Bajika in view of Nishibi, as applied to claim 17 above, and further in

view of Abburi (US Patent Publication 2003/0084306).

16.   As for claims 24 and 25, the system of Moshir and Bajika in view of Nishibi

discloses a method of sending the digital signature of the device to an authentication

server (i.e., …teaches signature information sent to the updated server). See Moshir,

paragraph 109. However, the system of Moshir and Bajika in view of Nishibi does not

specifically disclose wherein the authentication server allows a maximum number of

enrollments for a particular device. The Examiner respectfully contends at the time of

applicant's original filing, that prior art reference Abburi disclosed that a device will be

added to a device store on the synchronization server if it is determined that a maximum

number of devices have not yet been registered. (Paragraph 464, 471).

Therefore, to enhance the authentication process of Moshir and Bajika in view of

Nishibi, a person with ordinary skill in the art would have modified the system of Moshir

and Bajika in view of Nishibi with Abburi's capability to allow at the authentication server

a maximum number of device enrollments for a particular device.

17.   Claims 29 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Moshir and Bajika in view of Nishibi, as applied to claim 17 above, and further in

view of Hyman (US Patent 7,117,528).

18.   As for claims 29 and 30, the system of Moshir and Bajika in view of Nishibi

discloses the method of sending the digital signature of the device to an authentication

server (i.e., ...teaches signature information sent to the updated server). See Moshir, Paragraph 109. However, the system of Moshir and Bajika in view of Nishibi do not specifically disclose wherein multiple devices can be registered for a single user with the authentication server to create a registration hierarchy and wherein a user can unregister a device only through the device itself, or another device within the registration hierarchy registered earlier than the device to be unregistered. The Examiner respectfully contends that prior art reference Hyman discloses at the time of applicant's original filing that users of the client computers register with the authentication server for generating a user account (See Hyman fig 2; Col 7 lines 14-27; e.g. multiple devices can be registered for a single user with the authentication server) and that a new account is created and the old account is renamed (See Hyman, Col 10, lines 3-6; the new account is created and the old account is put into a ForceRename state).

Therefore, to enhance the registration capability of Moshir and Bajika in view of Nishibi, a person with ordinary skill in the would have modified the system of Moshir and Bajika in view of Nishibi with Hyman's capability to create a registration hierarchy to allow multiple device registration for a single user for authentication purposes.

Response to Arguments

Appellant's arguments, filed on 6/14/2010, with respect to the rejection(s) of claim(s) 17-35 are now considered to be moot in view of the new ground(s) of rejection.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's suforvisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431